3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.9.A1 Festlegung zulässiger Empfangender (B) [Zentrale Verwaltung]

Die zentrale Verwaltungsstelle MUSS sicherstellen, dass durch die Weitergabe von Informationen nicht gegen rechtliche Rahmenbedingungen verstoßen wird.

Die zentrale Verwaltungsstelle MUSS festlegen, wer welche Informationen erhalten und weitergeben darf. Es MUSS festgelegt werden, auf welchen Wegen die jeweiligen Informationen ausgetauscht werden dürfen. Alle Beteiligten MÜSSEN vor dem Austausch von Informationen sicherstellen, dass die empfangende Stelle die notwendigen Berechtigungen für den Erhalt und die Weiterverarbeitung der Informationen besitzt.

CON.9.A2 Regelung des Informationsaustausches (B)

Bevor Informationen ausgetauscht werden, MUSS die Institution festlegen, wie schutzbedürftig die Informationen sind. Sie MUSS festlegen, wie die Informationen bei der Übertragung zu schützen sind.

Falls schutzbedürftige Daten übermittelt werden, MUSS die Institution die Empfangenden darüber informieren, wie schutzbedürftig die Informationen sind. Falls die Informationen schutzbedürftig sind, MUSS die Institution die Empfangenden darauf hingewiesen werden, dass diese die Daten ausschließlich zu dem Zweck nutzen dürfen, zu dem sie übermittelt wurden.

CON.9.A3 Unterweisung des Personals zum Informationsaustausch (B) [Fachverantwortliche]

Fachverantwortliche MÜSSEN die Mitarbeitenden über die Rahmenbedingungen jedes Informationsaustauschs informieren. Die Fachverantwortlichen MÜSSEN sicherstellen, dass die Mitarbeitenden wissen, welche Informationen sie wann, wo und wie weitergeben dürfen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

CON.9.A4 Vereinbarungen zum Informationsaustausch mit Externen (S) [Zentrale Verwaltung]

Bei einem regelmäßigen Informationsaustausch mit anderen Institutionen SOLLTE die Institution die Rahmenbedingungen für den Informationsaustausch formal vereinbaren. Die Vereinbarung für den Informationsaustausch SOLLTE Angaben zum Schutz aller vertraulichen Informationen enthalten.

CON.9.A5 Beseitigung von Restinformationen vor Weitergabe (S) [Benutzende]

Zusätzlich zu den allgemeinen Schulungsmaßnahmen SOLLTE die Institution über die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien informieren. Es SOLLTE vermittelt werden, wie sie Rest- und Zusatzinformationen in Dokumenten und Dateien vermeiden werden können.

Die Institution SOLLTE Anleitungen bereitstellen, die vorgeben wie unerwünschte Restinformationen vom Austausch auszuschließen sind.

Jede Datei und jedes Dokument SOLLTE vor der Weitergabe auf unerwünschte Restinformationen überprüft werden. Unerwünschte Restinformationen SOLLTEN vor der Weitergabe aus Dokumenten und Dateien entfernt werden.

CON.9.A6 Kompatibilitätsprüfung des Sende- und Empfangssystems (S)

Vor einem Informationsaustausch SOLLTE überprüfen werden, ob die eingesetzten IT-Systeme und Produkte kompatibel sind.

CON.9.A7 Sicherungskopie der übermittelten Daten (S)

Die Institution SOLLTE eine Sicherungskopie der übermittelten Informationen anfertigen, falls die Informationen nicht aus anderen Quellen wiederhergestellt werden können.

CON.9.A8 Verschlüsselung und digitale Signatur (S)

Die Institution SOLLTE prüfen, ob Informationen während des Austausches kryptografisch gesichert werden können. Falls die Informationen kryptografisch gesichert werden, SOLLTEN dafür ausreichend sichere Verfahren eingesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

CON.9.A9 Vertraulichkeitsvereinbarungen (H) [Zentrale Verwaltung]

Bevor vertrauliche Informationen an andere Institutionen weitergeben werden, SOLLTE die zentrale Verwaltung informiert werden. Die zentrale Verwaltung SOLLTE eine Vertraulichkeitsvereinbarung mit der empfangenden Institution abschließen. Die Vertraulichkeitsvereinbarung SOLLTE regeln, wie die Informationen durch die empfangende Institution aufbewahrt werden dürfen. In der Vertraulichkeitsvereinbarung SOLLTE festgelegt werden, wer bei der empfangenden Institution Zugriff auf welche übermittelten Informationen haben darf.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) beschreibt in ihrem Standard *ISO/IEC 27001:2013*, Kap. 13.2 Anforderungen an den Austausch von Informationen.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.10 Entwicklung von Webanwendungen

1. Beschreibung

1.1. Einleitung

Webanwendungen bieten bestimmte Funktionen und dynamische (sich verändernde) Inhalte. Dazu stellen Webanwendungen auf einem Server Dokumente und Bedienoberflächen, z. B. in Form von Eingabemasken, bereit und liefern diese auf Anfrage an entsprechende Programme auf den Clients aus, z. B. an Webbrowser. Webanwendungen werden gewöhnlich auf der Grundlage von Frameworks (Rahmenstrukturen) entwickelt. Frameworks sind wiederverwendbare Programmschablonen für häufig wiederkehrende Aufgaben. Auch für Sicherheitskomponenten gibt es Frameworks.

Webanwendungen müssen Sicherheitsmechanismen umsetzen, die den Schutz der verarbeiteten Informationen gewährleisten und deren Missbrauch verhindern. Typische Sicherheitskomponenten bzw. -mechanismen sind Authentisierung, Autorisierung, Eingabevalidierung, Ausgabekodierung, Session-Management, Fehlerbehandlung und Protokollierung.

Die Entwickelnden müssen mit den relevanten Sicherheitsmechanismen einer Webanwendung vertraut sein. Aus diesem Grund hat der Entwicklungsprozess einen entscheidenden Einfluss auf die Sicherheit der späteren Software.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, sichere Webanwendungen zu entwickeln sowie Informationen zu schützen, die durch eine Webanwendung verarbeitet werden.

1.3. Abgrenzung und Modellierung

Der Baustein ist auf jedes Entwicklungsvorhaben im Informationsverbund anzuwenden, bei dem Webanwendungen entwickelt werden.

In diesem Baustein werden die spezifischen Gefährdungen und Anforderungen betrachtet, die bei der Entwicklung von Webanwendungen relevant sind. Anforderungen an den sicheren Einsatz von Webanwendungen werden nicht in diesem Baustein betrachtet. Sie sind im Baustein APP.3.1 *Webanwendungen und Webservices* zu finden. Ebenso werden allgemeine Anforderungen an die sichere Entwicklung von Software an anderer Stelle behandelt. Sie werden im Baustein CON.8 *Software-Entwicklung* behandelt.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.10 *Entwicklung von Webanwendungen* von besonderer Bedeutung.

2.1. Umgehung der Autorisierung bei Webanwendungen

Bei einem Angriff wird häufig versucht, auf Funktionen oder Daten von Webanwendungen zuzugreifen, die nur mit bestimmten Zugriffsrechten verfügbar sind. Ist die Autorisierung fehlerhaft umgesetzt, können unter Umständen die Berechtigungen eines anderen Kontos mit umfangreicheren Rechten erlangt werden und somit auf geschützte Bereiche und Daten zugegriffen werden. Dies geschieht beispielsweise, indem Eingaben gezielt manipuliert werden.

2.2. Unzureichende Eingabevalidierung und Ausgabekodierung

Verarbeitet eine Webanwendung ungeprüfte Eingabedaten, können möglicherweise Schutzmechanismen umgangen werden. Dieses Risiko erhöht sich, wenn gleichzeitig die Ausgabedaten der Webanwendung ohne ausreichende Kodierung direkt an den Webbrowser, die aufrufende Anwendung oder an nachgelagerte IT-Systeme übermittelt werden. Solche Ausgabedaten können Schadcode enthalten, der auf den Zielsystemen interpretiert oder ausgeführt wird. Beispielsweise kann bei einem Angriff Javascript Code in Formulardaten eingeben werden. Dieser Schadcode wird dann ungewollt vom IT-System ausgeführt, das die Webanwendung mit den Daten verarbeitet.

2.3. Fehlende oder mangelhafte Fehlerbehandlung durch Webanwendungen

Wenn während des Betriebs einer Webanwendung Fehler auftreten, die nicht korrekt behandelt werden, können sowohl der Betrieb einer Webanwendung als auch der Schutz ihrer Funktionen und Daten beeinträchtigt werden. Beispielsweise kann ein Fehler dazu führen, dass die Webanwendung nicht mehr korrekt ausgeführt wird und für Clients nicht mehr erreichbar ist. Außerdem werden unter Umständen Aktionen nur noch unvollständig durchgeführt, zwischengespeicherte Aktionen und Daten gehen verloren oder Sicherheitsmechanismen fallen aus.

2.4. Unzureichende Protokollierung von sicherheitsrelevanten Ereignissen

Wenn sicherheitsrelevante Ereignisse von der Webanwendung unzureichend protokolliert werden, können Sicherheitsvorfälle zu einem späteren Zeitpunkt nur schwer nachvollzogen werden. Die Ursachen für einen Vorfall sind dann möglicherweise nicht mehr ermittelbar. Beispielsweise können Konfigurationsfehler übersehen werden, wenn sie nicht zu Fehlermeldungen in den Log-Dateien führen. Auch Schwachstellen sind bei unzureichender Protokollierung schwer oder gar nicht zu erkennen und zu beheben.

2.5. Offenlegung sicherheitsrelevanter Informationen durch Webanwendungen

Webseiten und Daten, die von einer Webanwendung generiert und ausgeliefert werden, können Informationen zu den Hintergrundsystemen enthalten, z. B. Angaben zu Datenbanken oder Versionsständen von Frameworks. Diese Informationen können es erleichtern, gezielte Angriffe auf die Webanwendung durchzuführen.

2.6. Missbrauch einer Webanwendung durch automatisierte Nutzung

Wenn Funktionen einer Webanwendung automatisiert benutzt werden, können zahlreiche Vorgänge in kurzer Zeit ausgeführt werden. Mithilfe eines wiederholt durchgeführten Login-Prozesses kann bei einem Angriff z. B. versucht werden, gültige Kombinationen von Konten und Passwörtern zu erraten (Brute-Force). Außerdem können Listen mit gültigen Konten erzeugt werden (Enumeration), falls die Webanwendung Informationen über vorhandene Konten zurückgibt. Darüber hinaus können wiederholte Aufrufe von ressourcenintensiven Funktionen wie z. B. komplexen Datenbankabfragen für Denial-of-Service-Angriffe auf Anwendungsebene missbraucht werden.

2.7. Unzureichendes Session-Management von Webanwendungen

Unzureichendes Session-Management kann es ohne spezielle Zugriffsrechte ermöglichen, die Session-ID von Konten mit umfangreichen Zugriffsrechten zu ermitteln. Anschließend kann bei einem Angriff mit dieser ID auf geschützte Funktionen und Ressourcen der Webanwendung zugegriffen werden, z. B. in Form eines Session-Fixation-Angriffs. Hier wird zunächst eine Session-ID mit eingeschränkten Rechten von der Webanwendung beschafft. Diese ID wird, z. B. über einen Link in einer E-Mail, an höher legitimierte Personen übermittelt. Falls die höher legitimierten Personen diesem Link folgen und sich gegenüber der Webanwendung unter der Session-ID authentisieren, können Angreifende die Anwendung anschließend mit den vollen Zugriffsrechten der legitimen Konten verwenden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.10 *Entwicklung von Webanwendungen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Entwickelnde
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.10.A1 Authentisierung bei Webanwendungen (B)

Die Entwickelnden MÜSSEN sicherstellen, dass sich die Benutzenden gegenüber der Webanwendung sicher und angemessen authentisieren, bevor diese auf geschützte Funktionen oder Inhalte zugreifen können. Es MUSS eine angemessene Authentisierungsmethode ausgewählt werden. Der Auswahlprozess MUSS dokumentiert werden.

Eine zentrale Authentisierungskomponente MUSS verwendet werden. Die zentrale Authentisierungskomponente SOLLTE mit etablierten Standardkomponenten (z. B. aus Frameworks oder Programmbibliotheken) umgesetzt werden. Falls eine Webanwendung Authentisierungsdaten auf einem Client speichert, MUSS explizit auf die Risiken der Funktion hingewiesen werden und zustimmen („Opt-In“).

Die Webanwendung MUSS die Möglichkeit bieten, Grenzwerte für fehlgeschlagene Anmeldeversuche festzulegen. Die Webanwendung MUSS Benutzende sofort informieren, wenn deren Passwort zurückgesetzt wurde.

CON.10.A2 Zugriffskontrolle bei Webanwendungen (B)

Die Entwickelnden MÜSSEN mittels einer Autorisierungskomponente sicherstellen, dass die Benutzenden ausschließlich solche Aktionen durchführen können, zu denen sie berechtigt sind. Jeder Zugriff auf geschützte Inhalte und Funktionen MUSS kontrolliert werden, bevor er ausgeführt wird.

Die Autorisierungskomponente MUSS sämtliche Ressourcen und Inhalte berücksichtigen, die von der Webanwendung verwaltet werden. Ist die Zugriffskontrolle fehlerhaft, MÜSSEN Zugriffe abgelehnt werden. Es MUSS eine Zugriffskontrolle bei URL-Aufrufen und Objekt-Referenzen geben.

CON.10.A3 Sicheres Session-Management (B)

Session-IDs MÜSSEN geeignet geschützt werden. Session-IDs MÜSSEN zufällig und mit ausreichender Entropie erzeugt werden. Falls das Framework der Webanwendung sichere Session-IDs generieren kann, MUSS diese Funktion des Frameworks verwendet werden. Sicherheitsrelevante Konfigurationsmöglichkeiten des Frameworks MÜSSEN berücksichtigt werden. Wenn Session-IDs übertragen und von den Clients gespeichert werden, MÜSSEN sie ausreichend geschützt übertragen werden.

Eine Webanwendung MUSS die Möglichkeit bieten, eine bestehende Sitzung explizit zu beenden. Nachdem ein Konto angemeldet wurde, MUSS eine bereits bestehende Session-ID durch eine neue ersetzt werden. Sitzungen MÜSSEN eine maximale Gültigkeitsdauer besitzen (Timeout). Inaktive Sitzungen MÜSSEN automatisch nach einer bestimmten Zeit ungültig werden. Nachdem die Sitzung ungültig ist, MÜSSEN alle Sitzungsdaten ungültig und gelöscht sein.

CON.10.A4 Kontrolliertes Einbinden von Inhalten bei Webanwendungen (B)

Es MUSS sichergestellt werden, dass eine Webanwendung ausschließlich vorgesehene Daten und Inhalte einbindet ausliefert.

Die Ziele der Weiterleitungsfunktion einer Webanwendung MÜSSEN ausreichend eingeschränkt werden, sodass ausschließlich auf vertrauenswürdige Webseiten weitergeleitet wird. Falls die Vertrauensdomäne verlassen wird, MUSS ihn die Webanwendung darüber informieren.

CON.10.A5 Upload-Funktionen (B)

Die Entwickelnden MÜSSEN sicherstellen, dass die Benutzenden Dateien nur im vorgegebenen Pfad speichern können. Die Entwickelnden MÜSSEN sicherstellen, dass die Benutzenden den Ablageort der Uploads nicht beeinflussen kann. Die Entwickelnden MÜSSEN Funktionen in die Webanwendung integrieren, mit denen die Uploads während des Betriebs der Webanwendung konfiguriert werden können.

CON.10.A6 Schutz vor unerlaubter automatisierter Nutzung von Webanwendungen (B)

Die Entwickelnden MÜSSEN Sicherheitsmechanismen implementieren, die die Webanwendung vor automatisierten Zugriffen schützen. Bei der Implementierung der Sicherheitsmechanismen MUSS berücksichtigt werden, wie sich diese auf die Nutzungsmöglichkeiten der berechtigten Konten auswirken.

CON.10.A7 Schutz vertraulicher Daten (B)

Die Entwickelnden MÜSSEN sicherstellen, dass vertrauliche Daten von den Clients zu den Servern nur mit der HTTP-Post-Methode übertragen werden.

Entwickelnde MÜSSEN durch Direktiven in der Webanwendung gewährleisten, dass clientseitig keine schützenswerten Daten zwischengespeichert werden. Entwickelnde MÜSSEN sicherstellen, dass in Formularen keine vertraulichen Formulardaten im Klartext angezeigt werden. Die Webanwendung SOLLTE verhindern, dass vertrauliche Daten vom Webbrowser unerwartet gespeichert werden. Sämtliche Zugangsdaten der Webanwendung MÜSSEN serverseitig mithilfe von sicheren kryptografischen Algorithmen vor unbefugtem Zugriff geschützt werden (Salted Hash). Die Dateien mit den Quelltexten der Webanwendung MÜSSEN vor unerlaubten Abrufen geschützt werden.

CON.10.A8 Umfassende Eingabevalidierung und Ausgabekodierung (B)

Die Entwickelnden MÜSSEN sämtliche an eine Webanwendung übergebenen Daten als potenziell gefährlich behandeln und geeignet filtern. Sämtliche Eingabedaten sowie Datenströme und Sekundärdaten, wie z. B. Session-IDs, MÜSSEN serverseitig validiert werden.

Fehleingaben SOLLTEN möglichst nicht automatisch behandelt werden (Sanitizing). Lässt es sich jedoch nicht vermeiden, MUSS Sanitizing sicher umgesetzt werden.

Ausgabedaten MÜSSEN so kodiert werden, dass schadhafter Code auf dem Zielsystem nicht interpretiert oder ausgeführt wird.

CON.10.A9 Schutz vor SQL-Injection (B)

Falls Daten an ein Datenbankmanagementsystem (DBMS) weitergeleitet werden, MÜSSEN Stored Procedures bzw. Prepared SQL Statements eingesetzt werden. Falls Daten an ein DBMS weitergeleitet werden und weder Stored Procedures noch Prepared SQL Statements von der Einsatzumgebung unterstützt werden, MÜSSEN die SQL-Queries separat abgesichert werden.

CON.10.A10 Restriktive Herausgabe sicherheitsrelevanter Informationen (B)

Die Entwickelnden MÜSSEN sicherstellen, dass Webseiten, Rückantworten und Fehlermeldungen von Webanwendungen keine Informationen enthalten, die Angreifenden Hinweise darauf geben, wie er Sicherheitsmechanismen umgehen kann.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

CON.10.A11 Softwarearchitektur einer Webanwendung (S)

Die Entwickelnden SOLLTEN die Softwarearchitektur der Webanwendung mit allen Bestandteilen und Abhängigkeiten dokumentieren. Die Dokumentation SOLLTE bereits während des Entwicklungsverlaufs aktualisiert und angepasst werden. Die Dokumentation SOLLTE so gestaltet sein, dass sie schon in der Entwicklungsphase benutzt werden kann und Entscheidungen nachvollziehbar sind. In der Dokumentation SOLLTEN alle für den Betrieb notwendigen Komponenten gekennzeichnet werden, die nicht Bestandteil der Webanwendung sind. In der Dokumentation SOLLTE beschrieben sein, welche Komponenten welche Sicherheitsmechanismen umsetzen, wie die

Webanwendung in eine bestehende Infrastruktur integriert wird und welche kryptografischen Funktionen und Verfahren eingesetzt werden.

CON.10.A12 Verifikation essenzieller Änderungen (S)

Falls wichtige Einstellungen mit der Anwendung geändert werden sollen, dann SOLLTEN die Entwickelnden sicherstellen, dass die Änderungen durch die Eingabe eines Passworts erneut verifiziert werden. Falls dies nicht möglich ist, dann SOLLTE die Webanwendung auf andere geeignete Weise sicherstellen, dass sich die Benutzenden authentisieren. Die Benutzenden SOLLTEN über Änderungen mithilfe von Kommunikationswegen außerhalb der Webanwendung informiert werden.

CON.10.A13 Fehlerbehandlung (S)

Treten während der Laufzeit einer Webanwendung Fehler auf, SOLLTEN diese so behandelt werden, dass die Webanwendung weiter in einem konsistenten Zustand bleibt.

Die Webanwendung SOLLTE Fehlermeldungen protokollieren. Falls eine veranlasste Aktion einen Fehler verursacht, SOLLTE die Webanwendung diese Aktion abbrechen. Die Webanwendung SOLLTE im Fehlerfall den Zugriff auf eine angeforderte Ressource oder Funktion verweigern.

Zuvor reservierte Ressourcen SOLLTEN im Rahmen der Fehlerbehandlung wieder freigegeben werden. Der Fehler SOLLTE möglichst von der Webanwendung selbst behandelt werden.

CON.10.A14 Sichere HTTP-Konfiguration bei Webanwendungen (S)

Zum Schutz vor Clickjacking, Cross-Site-Scripting und anderen Angriffen SOLLTEN geeignete HTTP-Response-Header gesetzt werden. Es SOLLTEN mindestens die folgenden HTTP-Header verwendet werden: Content-Security-Policy, Strict-Transport-Security, Content-Type, X-Content-Type-Options sowie Cache-Control. Die verwendeten HTTP-Header SOLLTEN auf die Webanwendung abgestimmt werden. Die verwendeten HTTP-Header SOLLTEN so restriktiv wie möglich sein.

Cookies SOLLTEN grundsätzlich mit den Attributen *secure*, *SameSite* und *httponly* gesetzt werden.

CON.10.A15 Verhinderung von Cross-Site-Request-Forgery (S)

Die Entwickelnden SOLLTEN die Webanwendung mit solchen Sicherheitsmechanismen ausstatten, die eine Unterscheidung zwischen beabsichtigten Seitenaufrufen und unbeabsichtigt weitergeleiteten Befehlen Dritter ermöglichen. Dabei SOLLTE mindestens geprüft werden, ob neben der Session-ID ein geheimes Token für den Zugriff auf geschützte Ressourcen und Funktionen benötigt wird.

CON.10.A16 Mehr-Faktor-Authentisierung (S)

Es SOLLTE eine Mehr-Faktor-Authentisierung implementiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

CON.10.A17 Verhinderung der Blockade von Ressourcen (H)

Zum Schutz vor Denial-of-Service (DoS)-Angriffen SOLLTEN ressourcenintensive Operationen vermieden werden. Falls ressourcenintensive Operationen notwendig sind, dann SOLLTEN diese besonders abgesichert werden. Bei Webanwendungen SOLLTE ein möglicher Überlauf von Protokollierungsdaten überwacht und verhindert werden.

CON.10.A18 Kryptografische Absicherung vertraulicher Daten (H)

Vertrauliche Daten einer Webanwendung SOLLTEN durch sichere, kryptografische Algorithmen abgesichert werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Open Web Application Security Projekt stellt auf seiner Webseite Hinweise zur Absicherung von Webanwendungen zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Kryptographische Verfahren: Empfehlungen und Schlüssellängen: BSI TR-02102" Hinweise zur Anwendung kryptografischer Verfahren zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Entwicklung sicherer Webanwendungen" Hinweise zur Entwicklung sicherer Webanwendungen zur Verfügung.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellt im Dokument „Leitfaden zur Entwicklung sicherer Webanwendungen" Hinweise zur Entwicklung sicherer Webanwendungen durch Unternehmen zur Verfügung.

Bundesamt
für Sicherheit in der
Informationstechnik

CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

1. Beschreibung

1.1. Einleitung

Der staatliche Geheimschutz umfasst alle Maßnahmen zur Geheimhaltung von Informationen, die durch eine staatliche Stelle oder auf deren Veranlassung als Verschlusssachen (VS) eingestuft worden sind. VS sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform.

Der staatliche Geheimschutz wird durch Vorschriften des Bundes- und des Landesrechts geregelt. Rechtliche Grundlage für den staatlichen Geheimschutz des Bundes ist das Sicherheitsüberprüfungsgesetz (SÜG). Für den materiellen Geheimschutz des Bundes ist die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung, VSA) maßgeblich. Diese richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit VS arbeiten.

Wird Informationstechnik zur Handhabung von VS (VS-IT) eingesetzt, dann sind die Anforderungen der VSA zu beachten. Voraussetzung für den Einsatz von VS-IT ist ein Informationssicherheitskonzept nach den BSI-Standards des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung. Hinzu kommen die in diesem Baustein beschriebenen Anforderungen des Geheimschutzes, die über den IT-Grundschutz hinausgehen.

Unter Zusammenschaltung von VS-IT wird die direkte oder kaskadierte Verbindung von zwei oder mehr VS-IT-Systemen für die gemeinsame Nutzung von Daten und anderen Informationsressourcen (beispielsweise Kommunikation) bezeichnet.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, dass die Anforderungen des Geheimschutzes frühzeitig in den Informationssicherheitskonzepten berücksichtigt werden (Security-by-Design). Dieser Baustein soll die Geheimschutzbeauftragten dabei unterstützen, die Anforderungen der VSA für die elektronische Verarbeitung von VS bis zum Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) festzulegen und gemeinsam mit den Informationssicherheitsbeauftragten in das Informationssicherheitskonzept zu integrieren.

1.3. Abgrenzung und Modellierung

Der Baustein CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* ist einmal auf den gesamten Informationsverbund der VS-IT anzuwenden, falls VS des Geheimhaltungsgrades VS-NfD verarbeitet werden oder werden sollen. Dieser Baustein richtet sich an Bundesbehörden oder bundesunmittelbare öffentlich-rechtliche Einrichtungen, die der VSA unterliegen.

Falls der Baustein angewendet werden soll, dann ist zu beachten, dass dieser Baustein kein eigenständiges Regelwerk darstellt, sondern lediglich unterstützen soll, die VSA umzusetzen. Grundsätzlich ist zwischen Anforderungen zur Gewährleistung der Informationssicherheit und des Geheimschutzes zu unterscheiden. Der IT-Grundschutz dient der Umsetzung der Informationssicherheit und die VSA der Umsetzung des Geheimschutzes. Aus diesem Grund ersetzt eine ISO27001-Zertifizierung auf Basis von IT-Grundschutz nicht die Freigaben nach VSA. Um einen durchgehenden Geheimschutz umzusetzen, müssen die Anforderungen der VSA beachtet werden.

Die Anforderungen dieses Bausteins sind aus der VSA abgeleitet und behandeln folgende Aspekte:

- allgemeine Grundsätze der VSA,
- Zugang von Personen zu VS,
- VS-IT-Dokumentation,
- Handhabung elektronischer VS,
- Einsatz von VS-IT sowie
- Wartung und Instandhaltung von VS-IT.

Dabei bauen die Anforderungen dieses Bausteins auf den Anforderungen der Informationssicherheit auf und erweitern diese um die Anforderungen des Geheimschutzes. Um den betrachteten Informationsverbund mit VS-IT abzusichern und zu gewährleisten, dass die Informationssicherheit umgesetzt ist, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. Neben den relevanten System-Bausteinen wird unter anderem die Umsetzung der folgenden Prozess-Bausteine durch diesen Baustein vorausgesetzt, da diese um die Anforderungen des Geheimschutzes erweitert werden:

- ORP.1 *Organisation*,
- ORP.2 *Personal*,
- CON.6 *Löschen und Vernichten* sowie
- OPS.1.2.5 *Fernwartung*.

Dieser Baustein behandelt nicht:

- die Anforderungen der VSA, um VS-IT abzusichern, die für die Verarbeitung von VS der Geheimhaltungsgrade VS-VERTRAULICH oder höher eingesetzt werden sollen,
- die bauliche und technische Absicherung von Gebäuden und Räumen, in denen VS des Geheimhaltungsgrades VS-NfD verarbeitet werden, diese werden in den entsprechenden Bausteinen der Schicht INF *Infrastruktur* behandelt,
- die allgemeinen Anforderungen der VSA, die keinen unmittelbaren Bezug zu VS-IT haben sowie
- den Freigabeprozess für VS-IT.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* von besonderer Bedeutung.

2.1. Unbefugte Kenntnisnahme

Eine wesentliche Gefährdung des Geheimschutzes stellt die Kenntnisnahme von VS durch unbefugte Personen dar. Diese kann sich ergeben, wenn die Vorgaben der VSA nicht beachtet werden.

Beispiele:

- Die Einstufung und Kennzeichnung von VS unterbleibt, erfolgt falsch oder unvollständig.
- VS werden durch IT-Produkte gelöscht, die keine Zulassungsaussage besitzen.
- Die VS-IT-Dokumentation fehlt oder wird nur mangelhaft gepflegt.

Werden die Vorgaben der VSA nicht beachtet, kann dies dazu führen, dass

- bei einer fehlerhaften Handhabung von VS einige Geheimschutzmaßnahmen fälschlicherweise als nicht notwendig erachtet werden, wodurch diese nicht oder nicht im notwendigen Maße umgesetzt werden,
- VS so gelöscht werden, dass der Inhalt der VS wiederherstellbar ist,

- aufgrund einer fehlenden oder mangelhaften VS-IT-Dokumentation nicht nachvollzogen werden kann, ob ein erforderliches Geheimschutzniveau erreicht wird, in der Vergangenheit schon notwendige Maßnahmen zum Schutz der VS-IT getroffen wurden oder aktuell geplante Maßnahmen zu bereits umgesetzten Maßnahmen passen,
- VS mit einer IT verarbeitet werden, die keine ausreichenden Schutzmaßnahmen bietet.

Durch Anwendungen können Daten unbemerkt gespeichert oder vervielfältigt werden.

Beispiele:

- In Auslagerungsdateien oder Auslagerungspartitionen befinden sich mitunter schützenswerte Daten, z. B. Passwörter oder kryptografische Schlüssel.
- Bei der Verarbeitung von VS mit einem Textverarbeitungsprogramm können temporäre Arbeitskopien erzeugt werden, die unter bestimmten Umständen, beispielsweise nach einem Absturz des Programms, nicht gelöscht wurden.
- Auch fallen im laufenden Betrieb vieler Anwendungen Dateien an, die nicht für den produktiven Betrieb benötigt werden (z. B. Browserhistorie). Diese Dateien können sicherheitsrelevante Informationen enthalten.

Als Folge können solche Dateien ausgelesen werden, wenn die Datenträger ausgebaut und in ein anderes IT-System eingebaut werden. Wurden die Auslagerungs- oder Anwendungsdateien oder temporäre Dateien nicht sicher gelöscht, können Unbefugte Kenntnis von VS erlangen. Passwörter und Schlüssel können missbraucht werden, um unberechtigt auf VS-IT oder VS zuzugreifen.

Die Auswirkungen einer unbefugten Kenntnisnahme von VS des Geheimhaltungsgrad VS-NfD können für die Bundesrepublik Deutschland oder eines ihrer Länder von Nachteil sein. Diese können je nach Art der als VS eingestuften Informationen unterschiedlich ausfallen. Wenn beispielsweise eingestufte Netzpläne oder Informationssicherheitskonzepte offengelegt werden, dann können diese Informationen genutzt werden, um in IT-Systeme einzudringen. Erhalten Unbefugte beispielsweise Kenntnis von diplomatischen Informationen über ein anderes Land, dann kann dies die diplomatischen Beziehungen zwischen Deutschland und diesem Land belasten.

2.2. Konspirative Angriffe

Als konspirativer Angriff wird eine Form der Spionage bezeichnet, bei der Informationen verdeckt von nicht öffentlich zugänglichen Informationen durch ausländische Nachrichtendienste gewonnen werden. Bei konspirativen Angriffen möchten Nachrichtendienste möglichst unbemerkt an für sie interessante Informationen, wie z. B. VS, gelangen.

Bei konspirativen Beschaffungsaktivitäten verschleiern die Nachrichtendienste ihre wahren Absichten. Die Informationen werden über den Einsatz menschlicher Quellen (z. B. Social Engineering), durch technische Mittel (z. B. Abhörmaßnahmen oder Cyber-Angriffe, bei denen Hintertüren ausgenutzt oder Schadsoftware eingesetzt wird) oder durch eine Kombination beider Möglichkeiten beschafft.

In der Folge können ausländische Nachrichtendienste auf VS zugreifen und sich einen strategischen Vorteil gegenüber der Bundesrepublik Deutschland oder eines ihrer Länder verschaffen. Beispielsweise könnten andere Staaten diese Informationen nutzen, um ihre Verhandlungsposition gegenüber der Bundesrepublik Deutschland zu stärken. Auch andere Gruppierungen, wie beispielsweise terroristische Organisationen oder die organisierte Kriminalität, können mit den aus konspirativen Angriffen erlangten Informationen mögliche Aktivitäten effektiver planen und durchführen.

2.3. Angriffe durch Innentäter und -täterinnen

Bei einem Angriff durch sogenannte Innentäter und -täterinnen werden interne Informationen, wie z. B. VS, durch interne oder externe Mitarbeitende bewusst entwendet und gegebenenfalls an Dritte verkauft oder veröffentlicht. Innentäter und -täterinnen erfügen über ein breites Wissen über interne Prozesse und Arbeitsabläufe ihrer Institutionen. Darüber hinaus verfügen sie über Zutritts-, Zugangs- und Zugriffsrechte, über die Außenstehende nicht verfügen. Dieses Wissen und die ihnen für ihre dienstlichen Aufgaben erteilten Rechte können sie einsetzen, um die Erfolgswahrscheinlichkeit eines Angriffs zu erhöhen. Weiterhin können sie den Zeitpunkt des Angriffs so steuern, dass dieser durchgeführt wird, wenn dieser nur schwer erkannt werden kann, beispielsweise in Wartungsfenstern.

Die Ursachen, warum sich Mitarbeitende dazu entschließen Informationen zu entwenden, sind individuell unterschiedlich.

Beispiele:

- Die Innentäter und -täterinnen fühlen sich moralisch dazu verpflichtet, Informationen, die als VS eingestuft sind, zu veröffentlichen, um damit beispielsweise Missstände aufzudecken.
- Die Innentäter und -täterinnen wurden von einem Nachrichtendienst angeworben.
- Die Innentäter und -täterinnen möchten sich mit dem Verkauf von Informationen bereichern.

In der Folge können Dritte unberechtigt Zugang zu VS erlangen. Dies kann für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein. Die Voraussetzungen, unter denen ein Innentäter oder eine Innentäterin agiert, erschweren den Schutz vor einem solchen Angriff. Viele der zum Schutz vor Angriffen eingesetzten Maßnahmen sind gegen den Angriff durch einen Innentäter oder eine Innentäterin nicht wirksam.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins CON.11.1 *Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)* aufgeführt. Die Gesamtverantwortung für den Geheimschutz trägt die jeweilige Dienststellenleitung. Die damit verbundenen Aufgaben nimmt, sofern bestellt, der oder die jeweilige Geheimschutzbeauftragte war. Dieser oder diese ist für die Umsetzung der VSA zuständig. Wurde kein oder keine Geheimschutzbeauftragte bestellt, nimmt die Dienststellenleitung diese Aufgaben wahr. Der oder die Informationssicherheitsbeauftragte (diese Rolle entspricht der in der VSA und im UP Bund definierten Rolle der IT-Sicherheitsbeauftragten) unterstützt und berät den oder die Geheimschutzbeauftragte in allen Fragen zum Einsatz von VS-IT.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	Geheimschutzbeauftragte
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

Hinweis: Bei der Anwendung dieses Bausteins sind folgende Regelungen zu beachten:

- Dieser Baustein hat **keinerlei** Regelungscharakter. Es handelt sich **nicht** um ein eigenständiges Regelwerk, sondern die Anforderungen ergeben sich aus der VSA.
- Allgemeine Regelungen der VSA, die keine spezifischen Vorgaben zu VS-IT enthalten, sind **nicht** Bestandteil dieses Bausteins. Diese Regelungen sind der VSA zu entnehmen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

CON.11.1.A1 Einhaltung der Grundsätze zur VS-Verarbeitung mit IT nach § 3, 4 und 6 und Nr. 1 Anlage V zur VSA (B)

VS des Geheimhaltungsgrades VS-NfD DÜRFEN NUR mit VS-IT verarbeitet, die hierfür freigegeben ist. Private IT DARF NICHT für die Verarbeitung von Verschlusssachen eingesetzt werden. Bei der Verarbeitung von VS mit VS-IT MUSS der Grundsatz „Kenntnis nur, wenn nötig“ eingehalten werden. Es DÜRFEN NUR Personen Kenntnis von einer VS erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis erhalten müssen. Personen DÜRFEN NICHT umfassender oder eher über eine VS unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist.

Die Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig“ SOLLTE, insbesondere falls die VS-IT durch mehrere Benutzende verwendet wird, primär über technische Maßnahmen sichergestellt werden.

Nach dem Grundsatz der mehrschichtigen Sicherheit MÜSSEN personelle, organisatorische, materielle und technische Maßnahmen getroffen werden, die in ihrem Zusammenwirken

- Risiken eines Angriffs reduzieren (Prävention),
- Angriffe erkennbar machen (Detektion) und
- im Falle eines erfolgreichen Angriffs die negativen Folgen begrenzen (Reaktion).

Bei der Erfüllung der Anforderungen des vorliegenden Bausteins MÜSSEN die relevanten Technischen Leitlinien des BSI (BSI TL) beachtet werden. Falls von den BSI TL abgewichen werden soll, dann DARF dies NUR in Ausnahmefällen und im Einvernehmen mit dem BSI erfolgen.

CON.11.1.A2 Erstellung und Fortschreibung der VS-IT-Dokumentation nach § 12 und Nr. 2.2 Anlage II zur VSA (B)

Jede Dienststelle, die VS-IT einsetzt, MUSS als Teil der Geheimschutzdokumentation eine VS-IT-Dokumentation erstellen. Die VS-IT-Dokumentation MUSS alle Dokumente beinhalten, welche in Nr. 2.2 Anlage II zur VSA aufgeführt sind.

Die VS-IT-Dokumentation MUSS bei allen geheimschutzrelevanten Änderungen aktualisiert werden. Sie MUSS zudem mindestens alle drei Jahre auf Aktualität, Vollständigkeit und Erforderlichkeit bestehender und noch zu treffender Geheimschutzmaßnahmen überprüft werden.

CON.11.1.A3 Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA (B)

Auf Basis der im VS-Produktkatalog für einzelne Produkttypen vom BSI festgelegten Zulassungsrelevanz und insbesondere basierend auf den Ergebnissen der Strukturanalyse MÜSSEN alle für die geplante VS-IT relevanten IT-Sicherheitsfunktionen identifiziert werden. Diese lassen sich den folgenden Kategorien gemäß § 52 VSA zuordnen:

- Zugangs- und Zugriffskontrolle,
- Identifikation und Authentisierung,
- kryptographische Unterstützung,
- Sicherheitsmanagement,
- Informationsflusskontrolle,
- interner Schutz der Benutzerdaten,
- Selbstschutz der Sicherheitsfunktionen und ihrer Daten,
- Netztrennung,
- Schutz der Unversehrtheit,
- Verfügbarkeitsüberwachung oder
- Sicherheitsprotokollierung und Nachweisführung.

Anschließend MÜSSEN die identifizierten IT-Sicherheitsfunktionen den jeweiligen Teilkomponenten der VS-IT unter Berücksichtigung des VS-Produktkataloges des BSI zugeordnet werden. Jede identifizierte und für den Schutz von VS wesentlich verantwortliche Teilkomponente MUSS als IT-Sicherheitsprodukt gemäß VSA festgelegt und behandelt werden

Sofern das identifizierte IT-Sicherheitsprodukt einem Produkttyp angehört für das eine Zulassungsaussage gemäß BSI TL – IT 01 erforderlich ist, MUSS ein entsprechendes Produkt gemäß BSI Schrift 7164 (Liste der zugelassenen Produkte) verwendet werden. Sofern dort keine IT-Sicherheitsprodukte gelistet sind, MUSS Kontakt mit der Zulassungsstelle des BSI aufgenommen werden. Bei der Verwendung von IT-Sicherheitsprodukten mit Zulassungsaussage MÜSSEN zusätzlich die Bestimmungen des BSI für den Einsatz und Betrieb (SecOPs) des jeweiligen Produktes eingehalten werden.

CON.11.1.A4 Beschaffung von VS-IT nach § 49 VSA (B)

Bevor VS-IT beschafft wird, MUSS sichergestellt werden, dass deren Sicherheit während des gesamten Lebenszyklus ab dem Zeitpunkt, zu dem fest steht, dass die IT zur VS-Verarbeitung eingesetzt werden soll, bis zur Aussonderung

kontinuierlich gewährleistet wird. Um einen durchgehenden Geheimschutz sicherzustellen, MÜSSEN die Vergabeunterlagen so formuliert werden, dass die Anforderungen der VSA vollständig erfüllt werden können.

Bei Beschaffungsaufträgen für VS-IT MÜSSEN die notwendigen IT-Sicherheitsfunktionen der jeweiligen IT-Produkte vorab festgelegt werden. Bei der Formulierung der Vergabeunterlagen MÜSSEN insbesondere die

- Aufbewahrung,
- Archivierung und
- Löschung von elektronischer VS sowie
- Aussonderung,
- Wartung und Instandsetzung von VS-IT

berücksichtigt werden. Sofern einem zu beschaffenden IT-Produkt eine IT-Sicherheitsfunktion zugeordnet ist, SOLLTE ein IT-Produkt aus der Liste der zugelassenen IT-Sicherheitsprodukte beschafft werden. Wird stattdessen ein Produkt ohne Zulassungsaussage ausgewählt, dann SOLLTE im Vorhinein mit dem BSI abgeklärt werden, ob es zugelassen werden kann. Zusätzlich SOLLTE in der Ausschreibung aufgenommen werden, dass der Hersteller an einem Zulassungsverfahren mitwirken muss (siehe BSI TL – IT 01). Verträge MÜSSEN derart gestaltet werden, dass bei einer Rückgabe von defekten oder geleasten IT-Produkten deren Datenträger oder sonstige Komponenten, auf denen VS gespeichert sein könnten, im Besitz der Dienststelle verbleiben.

CON.11.1.A5 Verpflichtung bei Zugang zu VS nach § 4 VSA und Anlage V zur VSA (B)

Bevor eine Person Zugang zu VS des Geheimhaltungsgrades VS-NfD erhält, MUSS sie auf Anlage V verpflichtet werden. Ein Exemplar der Anlage V zur VSA MUSS jeder Person gegen Empfangsbestätigung zugänglich gemacht werden.

Wird Personal von nichtöffentlichen Stellen Zugang zu VS gewährt, so MUSS Nr. 6.6 Anlage V zur VSA beachtet werden. Von der Verpflichtung einer Person DARF NUR abgesehen werden, falls an VS-IT nur kurzzeitig gearbeitet und währenddessen ein Zugriff auf VS ausgeschlossen werden kann.

CON.11.1.A6 Beaufsichtigung und Begleitung von Fremdpersonal für VS-IT nach §§ 3, 4 VSA (B)

Nicht verpflichtetes Fremdpersonal, das an VS-IT arbeitet, MUSS während der gesamten Zeit begleitet und beaufsichtigt werden. Die begleitenden Personen MÜSSEN über die notwendigen Fachkenntnisse verfügen, um die Tätigkeiten kontrollieren zu können.

CON.11.1.A7 Kennzeichnung von elektronischen VS und Datenträgern nach §§ 20, 54 und Anlage III, V und VIII zur VSA (B)

Elektronische VS MÜSSEN nach den Vorgaben der VSA gekennzeichnet werden. Die Kennzeichnung MUSS bei der Verarbeitung von VS mit VS-IT während der gesamten Dauer ihrer Einstufung jederzeit erkennbar sein. Die Kennzeichnung MUSS auch bei kopierten, elektronisch versendeten oder ausgedruckten VS erhalten bleiben. Falls die Beschaffenheit elektronischer VS eine Kennzeichnung nach VSA nicht zulässt, dann MÜSSEN VS sinngemäß gekennzeichnet werden.

Der Dateiname einer elektronischen VS SOLLTE eine Kennzeichnung enthalten, die den VS-Charakter des Inhalts erkennen lässt, ohne die VS öffnen zu müssen. E-Mails MÜSSEN entsprechend des Musters 11 der Anlage VIII zur VSA gekennzeichnet werden.

Falls eine elektronische Kennzeichnung von VS (im Sinne von Metadaten) verwendet werden soll, dann MUSS geprüft werden, ob diese IT-Sicherheitsfunktionen übernimmt (siehe CON.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA)*.

Datenträger, auf denen elektronische VS des Geheimhaltungsgrades VS-NfD durch Produkte ohne Zulassungsaussage verschlüsselt gespeichert sind, MÜSSEN mit dem Geheimhaltungsgrad der darauf gespeicherten VS gekennzeichnet werden. Falls sich durch die Zusammenstellung der VS auf dem Datenträger ein Datenbestand ergibt, welcher eine höhere Einstufung erforderlich macht, dann MUSS der Datenträger selbst als VS des Geheimhaltungsgrades VS-VERTRAULICH behandelt und gekennzeichnet werden.

CON.11.1.A8 Verwaltung und Nachweis von elektronischen VS nach § 21 VSA (B)

Für die Verwaltung von elektronischen VS MÜSSEN die Grundsätze ordnungsgemäßer Aktenführung (gemäß Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien) und die Vorgaben der VSA zur Verwaltung und Nachweisführung von VS eingehalten werden (keine Nachweisführung für VS des Geheimhaltungsgrades VS-NfD erforderlich). Elektronische VS, die als VS-NfD eingestuft sind, DÜRFEN NUR unter Einhaltung des Grundsatzes „Kenntnis nur, wenn nötig" in offenen (elektronischen) Registraturen verwaltet werden.

CON.11.1.A9 Speicherung elektronischer VS nach § 23 und Nr. 5 Anlage V zur VSA (B)

Elektronische VS MÜSSEN mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt gespeichert oder entsprechend den Vorgaben der VSA materiell gesichert werden (siehe CON.11.1.A15 *Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA*).

CON.11.1.A10 Elektronische Übertragung von VS nach §§ 24, 53, 55 und Nr. 6.2 Anlage V zur VSA (B)

Falls VS elektronisch übertragen werden sollen, MÜSSEN die Regelungen der VSA zur Weitergabe von VS (§ 24 VSA) eingehalten werden. Für die Weitergabe an Parlamente, Landesbehörden und nicht öffentliche Stellen MÜSSEN zusätzlich die besonderen Regelungen nach §§ 25 und 26 VSA beachtet werden.

Die VS-IT aller Kommunikationspartner MUSS für die Verarbeitung von VS des Geheimhaltungsgrads VS-NfD freigegeben sein. Werden VS elektronisch übertragen, MÜSSEN sie grundsätzlich durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt werden. Auf eine Verschlüsselung DARF NUR verzichtet werden, falls:

- VS ausschließlich leitungsgebunden übertragen werden und die Übertragungseinrichtungen, einschließlich Kabel und Verteiler, gegen unbefugten Zugriff geschützt sind, oder
- neben den Hausnetzen zusätzlich das Transportnetz für die Verarbeitung von VS freigegeben ist.

Es DARF NUR innerhalb von Räumen und Bereichen, die gegen unkontrollierten Zutritt geschützt sind, von einem Zugriffsschutz ausgegangen werden.

VS DÜRFEN NUR in Ausnahmefällen nach § 55 Abs. 2-4 VSA unter Einhaltung der dort genannten Anforderungen und Vorsichtsmaßnahmen auf anderem Wege elektronisch übertragen werden. Falls im Vorhinein zu erwarten ist, dass VS elektronisch übertragen werden könnten, DARF die Ausnahmeregelung nach § 55 VSA NICHT angewendet werden.

CON.11.1.A11 Mitnahme elektronischer VS nach § 28 VSA und Nr. 7 Anlage V zur VSA (B)

Elektronische VS DÜRFEN NUR auf Dienstreisen und zu Dienstbesprechungen mitgenommen werden, soweit dies dienstlich notwendig ist und sie angemessen gegen unbefugte Kenntnisnahme gesichert werden. Werden diese persönlich mitgenommen, MÜSSEN diese folgendermaßen gespeichert werden:

- auf hierfür freigegebener VS-IT,
- auf einem Datenträger, der in einem verschlossenen Umschlag transportiert wird,
- auf einem Datenträger, der mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurde, oder
- durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt, falls der Datenträger selbst nicht durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurde.

Falls VS des Geheimhaltungsgrades VS-NfD in Privatwohnungen verarbeitet werden sollen, dann DÜRFEN diese NUR elektronisch mit hierfür freigegebener VS-IT verarbeitet werden.

CON.11.1.A12 Archivierung elektronischer VS nach §§ 30, 31 VSA (B)

VS MÜSSEN entsprechend dem Bundesarchivgesetz wie nicht eingestufte Informationen ausgesondert werden. Schon bei Einführung von Systemen zur elektronischen Schriftgutverwaltung und Vorgangsbearbeitung MÜSSEN die technischen Verfahren zur Aussonderung frühzeitig mit dem zuständigen Archiv abgesprochen werden. Falls das zuständige Archiv VS nicht übernehmen möchte, MÜSSEN VS gemäß CON.11.1.A13 *Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 VSA* sicher gelöscht bzw. vernichtet werden.

CON.11.1.A13 Löschung elektronischer VS, Vernichtung von Datenträgern und IT-Produkten nach §§ 32, 56 und Nr. 8 Anlage V zur VSA (B)

Um VS oder Datenträger zu löschen, die mit einem IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, MUSS der Schlüssel unter Beachtung der SecOPs gelöscht werden.

Sollen elektronische VS gelöscht werden, die nicht durch ein IT-Sicherheitsprodukt mit Zulassungsaussage verschlüsselt wurden, dann MUSS der gesamte Datenträger oder das IT-Produkt, auf dem VS gespeichert sind, mittels eines IT-Sicherheitsprodukts mit Zulassungsaussage gelöscht werden.

Die Datenträger oder IT-Produkte MÜSSEN gelöscht werden, bevor sie die gesicherte Einsatzumgebung dauerhaft verlassen. Sie MÜSSEN physisch vernichtet werden, falls sie nicht gelöscht werden können. Für die Vernichtung MÜSSEN Produkte oder Verfahren eingesetzt oder Dienstleister beauftragt werden, die die Anforderungen der BSI TL – M 50 erfüllen.

Die zuvor beschriebenen Teilanforderungen MÜSSEN auch bei defekten Datenträgern und IT-Produkten eingehalten werden.

CON.11.1.A14 Zugangs- und Zugriffsschutz nach § 3 VSA (B)

VS-IT, die für VS-NfD eingestufte VS eingesetzt wird, MUSS so geschützt werden, dass ein Zugang zur VS-IT und ein Zugriff auf VS nur für verpflichtete Personen (siehe CON.11.1.A5 *Verpflichtung bei Zugang zu VS nach § 4 und Anlage V zur VSA*) möglich ist. Der Schutz der VS MUSS sichergestellt werden über:

- IT-Sicherheitsprodukte mit Zulassungsaussage,
- materielle,
- organisatorische oder
- personelle Maßnahmen.

Für den Zugangs- und Zugriffsschutz SOLLTE eine Mehr-Faktor-Authentisierung genutzt werden.

CON.11.1.A15 Handhabung von Datenträgern und IT-Produkten nach § 54 und Anlage V zur VSA (B)

Datenträger und IT-Produkte MÜSSEN bei Nichtgebrauch in verschlossenen Behältern oder Räumen aufbewahrt werden, falls:

- der Datenträger bzw. das IT-Produkt selbst als VS-NfD eingestuft ist,
- auf dem Datenträger bzw. IT-Produkt unverschlüsselte VS des Geheimhaltungsgrades VS-NfD gespeichert sind oder
- auf dem Datenträger bzw. IT-Produkt VS des Geheimhaltungsgrades VS-NfD durch ein Produkt ohne Zulassungsaussage verschlüsselt gespeichert sind.

CON.11.1.A16 Zusammenschaltung von VS-IT nach § 58 VSA (B)

Bevor VS-IT mit anderer VS-IT zusammengeschaltet werden darf, MUSS geprüft werden, ob und inwieweit Informationen zwischen der zusammengeschalteten VS-IT ausgetauscht werden dürfen. Bei der Prüfung MUSS das jeweilige Schutzniveau und der Grundsatz „Kenntnis nur, wenn nötig“ berücksichtigt werden.

Abhängig vom Ergebnis der Prüfung MÜSSEN IT-Sicherheitsfunktionen zum Schutz der Systemübergänge implementiert werden (siehe CON.11.1.A3 *Einsatz von IT-Sicherheitsprodukten nach §§ 51, 52 VSA*). Vor der Zusammenschaltung der VS-IT MUSS bewertet und dokumentiert werden, ob diese für das angestrebte Szenario zwingend erforderlich ist und ob durch die Zusammenschaltung eine besondere Gefährdung der einzelnen Teilsysteme entsteht. Es MUSS geprüft werden, ob der durch die Zusammenschaltung von VS-IT entstandene Gesamtbestand der Daten höher einzustufen ist und weitere Geheimschutzmaßnahmen notwendig werden.

Wird VS-IT für die Verarbeitung von VS des Geheimhaltungsgrads VS-NfD direkt oder kaskadiert mit VS-IT für die Verarbeitung von VS des Geheimhaltungsgrades STRENG GEHEIM gekoppelt, dann MUSS sichergestellt werden, dass keine Verbindungen zu ungeschützten oder öffentlichen Netzen hergestellt werden.

CON.11.1.A17 Wartungs- und Instandsetzungsarbeiten von VS-IT nach § 3 Abs. 3 VSA (B)

Wartungs- und Instandsetzungsarbeiten an Komponenten der VS-IT SOLLTEN innerhalb der eigenen Dienstliegenschaft durchgeführt werden. Ist dies nicht möglich, MUSS sichergestellt werden, dass die Anforderungen der VSA sowohl während des Transports als auch bei den Wartungs- und Instandsetzungsarbeiten erfüllt werden.

Während der Wartungs- und Instandsetzungsarbeiten SOLLTE die Verarbeitung von VS in dem von der Wartung betroffenen Bereich der VS-IT eingestellt werden. Ist dies nicht möglich, MUSS während des Zeitraums der Wartungs- und Instandsetzungsarbeiten lückenlos sichergestellt werden, dass keine VS abfließen können.

Nach Abschluss der Wartungs- und Instandsetzungsarbeiten MUSS der oder die Geheimschutzbeauftragte bewerten, ob sich geheimschutzrelevante Änderungen an der VS-IT ergeben haben.

CON.11.1.A18 Fernwartung von VS-IT nach § 3 Abs. 3 VSA (B)

Wird VS-IT ferngewartet, dann MUSS die Fernwartungsverbindung verschlüsselt sein. Für die Verschlüsselung MÜSSEN IT-Sicherheitsprodukte mit Zulassungsaussage eingesetzt werden.

Die IT, mit der die Fernwartung durchgeführt wird, sowie die Übertragungsstrecken MÜSSEN als VS-IT behandelt und als Schutzobjekte definiert werden.

Die Fernwartungsverbindung MUSS durch die Dienststelle auf- und abgebaut werden. Die Dienststelle MUSS in der Lage sein, die Verbindung bei Auffälligkeiten auch während der Wartung zu unterbrechen.

Für die Fernwartung von VS-IT MUSS ein Informationssicherheitskonzept erstellt werden, das alle Komponenten, die an der Fernwartung beteiligt sind, berücksichtigt. Hierbei MÜSSEN insbesondere die Netzübergänge und die VS-IT, aus dem die Fernwartung gesteuert wird, betrachtet werden.

3.2. Standard-Anforderungen

Für diesen Baustein sind keine Standard-Anforderungen definiert.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Gesetzliche Grundlage für den Geheimschutz bildet das „Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen (Sicherheitsüberprüfungsgesetz – SÜG).

Die auf der Grundlage des SÜG erlassene „Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA)“ enthält die Vorgaben für den materiellen Geheimschutz in der Bundesverwaltung.

Das BMWK veröffentlicht für den nichtöffentlichen Bereich das Geheimschutzhandbuch der Wirtschaft (GHB).

Das BSI gibt zur Umsetzung der VSA Technische Leitlinien heraus.

Das BSI gibt mit der „BSI-Schrift 7164“ eine Liste heraus, die alle IT-Sicherheitsprodukte mit gültiger Zulassungsaussage auflistet.

Weitergehende Informationen zur Zulassung von IT-Sicherheitsprodukten und einer genaueren Beschreibung der einzelnen IT-Sicherheitsfunktionen bietet das Dokument „VS-Produktkatalog des BSI“.

Die Grundsätze ordnungsgemäßer Aktenführung sind in der „Registraturrichtlinie für das Bearbeiten und Verwalten von Schriftgut in Bundesministerien“, die vom BMI herausgegeben wird, festgelegt.

OPS: Betrieb

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.1 Allgemeiner IT-Betrieb

1. Beschreibung

1.1. Einleitung

Der IT-Betrieb (engl. IT Operations) stellt eine Organisationseinheit und den zugehörigen Geschäftsprozess innerhalb der Informationstechnik dar. Der Prozess beschreibt die Aufgaben mit allen Tätigkeiten, die durch die Organisationseinheit IT-Betrieb umgesetzt werden. Die IT umfasst alle IT-Komponenten einer Institution, insbesondere IT-Systeme, -Dienste, -Anwendungen, -Plattformen und Netze. Zum IT-Betrieb zählen unter anderem die folgenden Aufgaben:

- die Verwaltung, inklusive Inventarisierung und Dokumentation
- die Mitwirkung bei der Beschaffung
- die In- und Außerbetriebnahme, inklusive Austausch von IT
- die IT-Administration
- das IT-Monitoring
- das IT Incident Management

Die ordnungsgemäße, sichere und korrekte Ausführung des IT-Betriebs ist unabdingbar, um die Funktionsfähigkeit der IT zu gewährleisten. Hierzu legt der IT-Betrieb Rahmenbedingungen beispielsweise für die Prozessgestaltung fest und stellt sicher, dass diese eingehalten werden.

Außerdem muss der IT-Betrieb auch die eigenen verwendeten Betriebsmittel, also die spezifischen IT-Komponenten, die für betriebliche Zwecke des IT-Betriebs eingesetzt werden, in angemessenem Umfang zur Verfügung stellen und deren Funktionsfähigkeit gewährleisten. Die betriebene IT umfasst also immer auch die Betriebsmittel des IT-Betriebs selbst. Diesen Betriebsmitteln kommt aus Sicherheitsperspektive eine besondere Bedeutung zu. Auf ihnen werden viele für die IT-Komponenten und deren Funktionsfähigkeit wichtige Informationen vorgehalten, die ein attraktives Ziel für einen Angriff bieten und daher geschützt werden müssen. Außerdem ist ihre Verfügbarkeit für den IT-Betrieb wesentlich.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei allen allgemein gültigen Aspekten des IT-Betriebs zu etablieren. Mit der Umsetzung dieses Bausteins sorgt die Institution dafür, dass die Tätigkeiten des allgemeinen IT-Betriebs, durch die die Funktionsfähigkeit der IT sichergestellt wird, ordnungsgemäß und systematisch durchgeführt werden.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.1 *Allgemeiner IT-Betrieb* ist einmal auf den gesamten Informationsverbund anzuwenden.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt übergreifende Aspekte des IT-Betriebs. In größeren Institutionen ist es sinnvoll, darüber hinaus den IT-Betrieb in das Service-Management der Institution einzubetten. Hierzu können Standardwerke, wie z. B. die „Information Technology Infrastructure Library“ (ITIL), herangezogen werden. Ein solches Service Management ist nicht auf die IT beschränkt (IT-Service-Management), sondern adressiert auch Geschäftsprozesse und Fachaufgaben wie „Portfolio Management“.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- spezielle Aspekte des IT-Betriebs aus weiteren Bausteinen der Schicht OPS.1.1 *Kern-IT-Betrieb,* insbesondere die Durchführung der Administration (siehe OPS.1.1.2 *Ordnungsgemäße IT-Administration*) und Tätigkeiten im Patch- und Änderungsmanagement (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- Aspekte des Netz- und Systemmanagements (siehe NET.1.2 *Netzmanagement* und OPS.1.1.7 *Systemmanagement*)
- die ordnungsgemäße Verwaltung von Benutzenden und Rechten (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)
- Aspekte der Datensicherung und Archivierung (siehe CON.3 *Datensicherungskonzept* und OPS.1.2.2 *Archivierung*)
- Aspekte, die sich nicht auf den Regelbetrieb, sondern auf Ausnahmesituationen beziehen, insbesondere auf einen IT-Angriff und die Kompromittierung von IT-Systemen (Incident Management, siehe Baustein DER.1 *Detektion von sicherheitsrelevanten Ereignissen* sowie Bausteine aus dem Bereich DER.2 *Security Incident Management* und Baustein DER.4 *Notfallmanagement*)
- besondere Anforderungen für den Fall, dass der IT-Betrieb durch Dritte erfolgt (siehe OPS.2.3 *Nutzung von Outsourcing* und OPS.3.2 *Anbieten von Outsourcing*)

Dieser Baustein behandelt **nicht**

- den Teil des Betriebs von IT-Komponenten, für den nicht der IT-Betrieb, sondern z. B. eine Fachabteilung zuständig ist,
- spezielle Aspekte von DevOps,
- Aspekte, die kennzeichnend für den IT-Service sind, beispielsweise die Schnittstelle zu Benutzenden oder die Bereitstellung einer Hotline, sowie
- die Umsetzung von IT-Projekten.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.1 *Allgemeiner IT-Betrieb* von besonderer Bedeutung.

2.1. Unzureichende Personalkapazitäten

Das Betriebspersonal ist dafür zuständig, dass die gesamte IT funktionsfähig ist, ohne die Institutionen häufig nicht mehr operabel sind. Die IT ist besonders gefährdet, falls der IT-Betrieb nicht über ausreichende Kapazitäten verfügt.

Herrscht Personalmangel, z. B. aufgrund fehlerhafter oder unzureichender Personalplanung, können Prozesse des IT-Betriebs nicht ordnungsgemäß ausgeführt werden. Dabei können neben der Verfügbarkeit auch die Vertraulichkeit und Integrität des Informationsverbundes eingeschränkt werden, z. B. wenn aufgrund von Personalmangel kein geeignetes IT-Monitoring oder Security Monitoring erfolgt.

Ist das benötigte Know-how beim Betriebspersonal nicht ausreichend redundant verfügbar, da weiteres Personal beispielsweise nur unzureichend geschult wurde, kann die Abhängigkeit von einzelnen Personen dazu führen, dass die Verfügbarkeit des IT-Betriebs nicht mehr vollständig gewährleistet ist.

2.2. Verlust betriebsrelevanter Informationen

Prozesse, die durch den IT-Betrieb unzureichend ausgeführt werden, können dazu führen, dass betriebsrelevante Informationen veraltet sind oder gar verloren gehen.

Führt der IT-Betrieb Tätigkeiten aus, die auf einer unzureichenden oder manipulierten Dokumentation basieren, kann dies zu Störungen der IT-Funktionalität führen. Sind darüber hinaus die Informationen, die benötigt werden um einen Störfall zu beheben, nur unzureichend vorhanden, können diese Störungen nicht oder nur fehlerhaft behoben werden. Als Folge unzureichender Dokumentation kann sowohl die Verfügbarkeit der IT-Komponenten als auch die Vertraulichkeit der Informationen beeinträchtigt werden.

Werden die betriebsrelevanten Informationen unzureichend abgesichert, z. B. indem sie offengelegt oder leicht zugänglich sind, ist deren Vertraulichkeit nicht mehr gewährleistet.

Eine Ursache für den Verlust betriebsrelevanter Informationen kann z. B. eine unzureichende Abstimmung mit den beauftragten Dienstleistenden über die zu liefernde Dokumentation sein, was in den oben genannten Konsequenzen resultieren kann.

2.3. Eingeschränkte Verfügbarkeit von Betriebsmitteln

Betriebsmittel, worunter sämtliche IT-Komponenten zusammengefasst werden, mit denen die Tätigkeiten des IT-Betriebs erbracht werden, haben einen erheblichen Einfluss darauf, dass IT-Betriebsprozesse effizient durchgeführt werden können.

Sind die Betriebsmittel unzureichend redundant ausgelegt, nur eingeschränkt gehärtet oder überlastet, kann hierdurch die Verfügbarkeit eingeschränkt sein. Falls Betriebsmittel nicht ausreichend verfügbar sind, können z. B. aufgetretene Fehler an betriebenen IT-Komponenten nicht behoben werden, wodurch die Verfügbarkeit, Integrität oder Vertraulichkeit der betriebenen IT-Komponenten gefährdet wird.

2.4. Missbrauch betriebsrelevanter Informationen und privilegierter Rechte durch berechtigte Personen

Privilegierte Rechte des Betriebspersonals ermöglichen weitreichende Auswirkungen auf die gesamte IT. Werden betriebsrelevante Informationen und privilegierte Rechte durch berechtigte Personen missbraucht, um zu sabotieren, zu manipulieren oder Informationen auszuspähen, sind alle Schutzziele der Informationssicherheit für die betriebenen IT-Komponenten und für die Informationen der Institution gefährdet. Diese Ausgangslage kann mehrere Ursachen haben.

Verfügt das Betriebspersonal über zu weit gefasste privilegierte Rechte, können diese Berechtigungen für Angriffe missbraucht werden. Auch kann durch Nötigung, Phishing oder Social Engineering erzwungen werden, dass weitreichende Rechte freigegeben oder betriebsrelevante Informationen preisgegeben werden.

Wenn internes oder externes Betriebspersonal ausscheidet und die entsprechenden Prozesse unzureichend ausgeführt werden, können solche Personen weiterhin die privilegierten Rechte nutzen. Ebenso können Sammel-Accounts bewirken, dass z. B. beim Wechsel des Arbeitsfeldes weiterhin Zugang zu betriebsrelevanten Informationen und Betriebsmitteln gewährt wird.

Betriebsrelevante Informationen können auch durch menschliche Fehler preisgegeben werden, indem beispielsweise Regelungen nicht umgesetzt werden, die Ausspähung oder Diebstahl verhindern.

2.5. Erreichbarkeit oder Ausspähen von Betriebsmitteln und betriebsrelevanten Informationen durch Unbefugte

Besteht kein ausreichender Schutz gegen unbefugte Zutritte zu Räumlichkeiten, in denen Betriebsmittel positioniert sind, kann dies als Ausgangspunkt für jede Art von Angriffen bzw. Missbrauch ausgenutzt werden. Folglich können alle Schutzziele der Informationssicherheit beeinträchtigt werden.

Schnittstellen bzw. Zugänge des IT-Betriebs, die unzureichend abgesichert werden, können begünstigen, dass unbefugte Personen Betriebsmittel und betriebsrelevante Informationen erreichen oder ausspähen können.

2.6. Fehlleiten des IT-Betriebs

Spiegeln interne oder externe Personen dem IT-Betrieb bewusst falsche Tatsachen vor, indem sich diese z. B. fälschlicherweise als andere Person ausgeben, kann der IT-Betrieb zu falschen Reaktionen verleitet werden. Dabei können z. B. Phishing E-Mails, die an den IT-Betrieb gesendet werden, inkorrekte Tätigkeiten auslösen. Abhängig davon, wie der IT-Betrieb fehlgeleitet wird, können alle Schutzziele der Informationssicherheit erheblich gefährdet werden. Die Verfügbarkeit kann eingeschränkt werden, wenn zum Beispiel die Administrierenden dazu verleitet werden, IT-Systeme auszuschalten.

2.7. Verhinderung von Betriebsprozessen

Werden die Tätigkeiten des IT-Betriebs blockiert und somit nicht ordnungsgemäß ausgeführt, kann hierdurch die Verfügbarkeit und die Integrität der gesamten IT beeinträchtigt werden.

Eine mögliche Ursache kann eine unzureichende Konzeptionierung und Beschaffung von IT-Komponenten sein, indem z. B. nicht berücksichtigt wurde, ob die Anwendungen gut betrieben werden können. Ebenso kann die Fehlplanung von Prozessen, z. B. durch unklare Schnittstellen oder Zuständigkeiten, dazu führen, dass der IT-Betrieb nur unzureichend ausgeführt wird.

Auch inkorrekt ausgeführte Tätigkeiten des Betriebspersonals, die z. B. auf unzureichendes Know-how über Betriebsprozesse zurückzuführen sind, können bewirken, dass Betriebsprozesse verhindert werden und dadurch die gesamte IT nur noch eingeschränkt verfügbar bzw. funktionstüchtig ist.

Ebenso kann das Verhalten des Betriebspersonals oder die Tätigkeiten von verschiedenen Dienstleistenden mit nicht klar abgegrenzten Schnittstellen verhindern, dass Betriebsprozesse korrekt ausgeführt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.1 *Allgemeiner IT-Betrieb* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.1.A1 Festlegung der Aufgaben und Zuständigkeiten des IT-Betriebs (B)

Für alle betriebenen IT-Komponenten MUSS festgelegt werden, welche Aufgaben für den IT-Betrieb anfallen und wer dafür zuständig ist. Hierfür MÜSSEN die entsprechenden Rechte, Pflichten, Aufgaben mit den hierfür erforderlichen Tätigkeiten, Befugnisse und zugehörigen Prozesse geregelt werden. Weiterhin MÜSSEN die Schnittstellen und Meldewege sowie das Eskalationsmanagement zwischen verschiedenen Betriebseinheiten und gegenüber anderen organisatorischen Einheiten der Institution festgelegt werden.

OPS.1.1.1.A2 Festlegung von Rollen und Berechtigungen für den IT-Betrieb (B)

Für alle betriebenen IT-Komponenten MUSS das jeweilige Rollen- und Berechtigungskonzept auch Rollen und zugehörige Berechtigungen für den IT-Betrieb festlegen. Für die Betriebsmittel MUSS ebenfalls ein Rollen- und Berechtigungskonzept erstellt werden.

Das Rollen- und Berechtigungskonzept für den IT-Betrieb MUSS die IT-Nutzung von IT-Betriebsaufgaben trennen. Administrationsaufgaben und sonstige Betriebsaufgaben MÜSSEN durch unterschiedliche Rollen getrennt werden. Grundsätzlich SOLLTE der IT-Betrieb für unterschiedliche Betriebstätigkeiten unterschiedliche Rollen festlegen, die für die jeweiligen Tätigkeiten die erforderlichen Berechtigungen besitzen. Sammel-Accounts DÜRFEN NUR in begründeten Ausnahmefällen eingerichtet werden.

Die Rollen und Berechtigungen MÜSSEN regelmäßig geprüft und auf die aktuellen Gegebenheiten angepasst werden. Insbesondere MÜSSEN die Berechtigungen von ausgeschiedenem Personal auf den IT-Komponenten entfernt werden. Ebenso MÜSSEN die Rollen und Berechtigungen gelöscht werden, wenn IT-Komponenten außer Betrieb genommenen werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.1.A3 Erstellen von Betriebshandbüchern für die betriebene IT (S)

Für alle betriebenen IT-Komponenten SOLLTEN die Betriebsaufgaben geplant und in Betriebshandbüchern erfasst werden. Die Betriebshandbücher SOLLTEN stets verfügbar sein und mindestens die folgenden Themen adressieren:

- relevante System- und Kontaktinformationen
- erforderliche und zulässige Betriebsmittel
- allgemeine Konfigurationsvorgaben
- Konfigurationsvorgaben zur Härtung von Spezialsystemen
- Rollen- und Berechtigungen
- IT-Monitoring, Protokollierung und Alarmierung
- Datensicherung und Notfallkonzepte
- IT Incident Management
- Vorgaben für alle regelmäßigen und außerplanmäßigen Tätigkeiten

Die Betriebshandbücher SOLLTEN regelmäßig und anlassbezogen geprüft und angepasst werden.

OPS.1.1.1.A4 Bereitstellen ausreichender Personal- und Sachressourcen (S)

Der IT-Betrieb SOLLTE über ausreichende Personal-Ressourcen verfügen, um einen ordnungsgemäßen IT-Betrieb gewährleisten zu können. Hierfür SOLLTE der Aufwand für alle Tätigkeiten des IT-Betriebs ermittelt werden. Die Personal-Ressourcen SOLLTEN mit angemessenen Redundanzen und Reserven geplant werden und auch kurzfristige Personalausfälle sowie temporär erhöhte Personalbedarfe berücksichtigen.

Ebenfalls SOLLTEN geeignete Sach-Ressourcen bereitstehen. Hierfür SOLLTE für jede Tätigkeit des IT-Betriebs identifiziert werden, welche Betriebsmittel erforderlich sind.

Die Ressourcenplanung SOLLTE regelmäßig und anlassbezogen überprüft und an die aktuellen Erfordernisse angepasst werden.

OPS.1.1.1.A5 Festlegen von gehärteten Standardkonfigurationen (S)

Der IT-Betrieb SOLLTE die betriebenen IT-Komponenten kategorisieren und für diese Kategorien gehärtete Standardkonfigurationen festlegen und bereitstellen.

Für IT-Plattformen wie Virtualisierungshosts, auf denen weitere IT-Komponenten bereitgestellt und betrieben werden, SOLLTE eine abgestimmte Härtung entwickelt und umgesetzt werden, die alle Elemente der IT-Komponenten berücksichtigt. Hierbei SOLLTEN verschiedene Ausprägungen der IT-Komponenten berücksichtigt und erlaubte Abweichungen spezifiziert werden.

Die Konfigurationsvorgaben SOLLTEN die Sicherheitsanforderungen der Institution umsetzen und die Empfehlungen der jeweiligen Herstellenden berücksichtigen. Die gehärteten Standard-Konfigurationen SOLLTEN in den jeweiligen Betriebshandbüchern dokumentiert werden.

Jede Standardkonfiguration SOLLTE vor Bereitstellung getestet werden. Die gehärteten Standardkonfigurationen SOLLTEN regelmäßig und anlassbezogen geprüft und gemäß der verfügbaren Informationen an den aktuellen Stand der Technik angepasst werden.

Der IT-Betrieb SOLLTE gewährleisten, dass die aktuellen Konfigurationsvorgaben stets verfügbar sind und über eine Versionierung und eine Beschreibung identifizierbar sind.

OPS.1.1.1.A6 Durchführung des IT-Asset-Managements (S)

Der IT-Betrieb SOLLTE eine Übersicht aller vorhandenen IT-Assets erstellen, regelmäßig prüfen und aktuell halten.

Im IT-Asset-Management (ITAM) SOLLTEN alle produktiven IT-Komponenten, Test-Instanzen und IT-Komponenten der Reservevorhaltung erfasst werden. Auch vorhandene, aber nicht mehr genutzte IT-Assets SOLLTEN erfasst werden.

Es SOLLTEN ITAM-Tools eingesetzt werden, die eine zentrale Verwaltung der IT-Assets ermöglichen.

OPS.1.1.1.A7 Sicherstellung eines ordnungsgemäßen IT-Betriebs (S)

Der IT-Betrieb SOLLTE für alle IT-Komponenten Betriebskonzepte entwickeln. Diese Betriebskonzepte SOLLTEN regelmäßig geprüft und angepasst werden.

Die sicherheitsrelevanten Vorgaben zur Konfiguration SOLLTEN umgesetzt werden. Dafür SOLLTEN die gehärteten Standard-Konfigurationen genutzt werden.

Der IT-Betrieb SOLLTE für alle Tätigkeiten Prüfkriterien festlegen, die in ihrer Gesamtheit als Leitfaden für den ordnungsgemäßen IT-Betrieb dienen. Die Freigabe von installierten oder geänderten IT-Komponenten in den produktiven Betrieb SOLLTE über diese Prüfkriterien nachgewiesen werden.

Bei Inbetriebnahme und nach Updates oder Umstrukturierungen SOLLTEN Systemtests für die IT-Komponenten durchgeführt werden. Der IT-Betrieb SOLLTE festlegen, in welcher Umgebung die jeweiligen Systemtests mit welcher Testabdeckung und Testtiefe durchgeführt werden.

Der IT-Betrieb SOLLTE Vorkehrungen für die Ersatzbeschaffung von IT-Komponenten treffen. Hierfür SOLLTEN eine Reservevorhaltung oder Lieferverträge vorgesehen werden.

Alle Tätigkeiten des IT-Betriebs SOLLTEN umfassend und nachvollziehbar erfasst werden. Hierfür SOLLTE der IT-Betrieb ein geeignetes Werkzeug wie ein Ticketsystem nutzen.

Der IT-Betrieb SOLLTE insbesondere die Qualität der Betriebsprozesse, die Einhaltung von SLAs und die Zufriedenheit der Benutzenden systematisch erfassen. Es SOLLTEN regelmäßig Reports erstellt werden, die dem Nachweis eines ordnungsgemäßen IT-Betriebs dienen.

OPS.1.1.1.A8 Regelmäßiger Soll-Ist-Vergleich (S)

Der IT-Betrieb SOLLTE regelmäßig und anlassbezogen für alle betriebenen IT-Komponenten sowie für die Betriebsmittel prüfen, ob die aktuelle Konfiguration dem Sollzustand entspricht. Darüber hinaus SOLLTE geprüft werden, ob die gelebten Prozesse die festgelegten Prozesse des IT-Betriebs umsetzen.

OPS.1.1.1.A9 Durchführung von IT-Monitoring (S)

Alle IT-Komponenten SOLLTEN in ein einheitliches IT-Monitoring eingebunden werden, das alle relevanten Parameter der IT-Komponenten beinhaltet. Das IT-Monitoring SOLLTE mit dem übergeordneten Service-Management abgestimmt werden.

Der IT-Betrieb SOLLTE das IT-Monitoring entsprechend eines vorher festgelegten Monitoring-Plans durchführen. Je IT-Komponente SOLLTEN angemessene Schwellwerte ermittelt werden, die eine Meldung oder einen Alarm auslösen.

Der IT-Betrieb SOLLTE für das IT-Monitoring spezifizieren, welche Meldewege genutzt werden und welche Konsequenzen aus den Meldungen oder Alarmen gezogen werden. Auf Basis von Monitoring-Ergebnissen SOLLTE überprüft werden, ob die Infrastruktur erweitert oder angepasst wird. Über die gewonnenen Erkenntnisse SOLLTEN regelmäßig Reports erstellt werden, die das aktuelle Lagebild der betriebenen IT und die zeitliche Entwicklung sowie Trends darstellen.

Die Konzeption des IT-Monitorings SOLLTE regelmäßig und anlassbezogen geprüft und aktualisiert werden, um dem aktuellen Stand der Technik und der betriebenen Infrastruktur zu entsprechen.

Die Monitoring-Daten SOLLTEN nur über sichere Kommunikationswege übertragen werden.

OPS.1.1.1.A10 Führen eines Schwachstelleninventars (S)

Der IT-Betrieb SOLLTE ein Schwachstelleninventar führen, in dem die Schwachstellen aller betriebenen IT-Komponenten und der Umgang mit diesen zentral erfasst und gepflegt werden.

Der IT-Betrieb SOLLTE die Behandlung der Schwachstellen initiieren, nachhalten und sicherstellen. Es SOLLTE ein Prozess definiert werden, der den Umgang mit den Schwachstellen festlegt. Mindestens SOLLTE spezifiziert werden,

- bis wann ein verfügbares Update, in dem die Schwachstelle behoben ist, zu installieren ist,
- in welchen Fällen und bis wann IT-Komponenten mit Schwachstellen außer Betrieb genommen oder ersetzt werden und
- ob und wie solche IT-Komponenten separiert werden, falls weder ein Ersatz noch ein Update möglich ist.

OPS.1.1.1.A11 Festlegung und Einhaltung von SLAs (S)

Für alle IT-Komponenten und alle Tätigkeiten SOLLTE der IT-Betrieb Service Level Agreements (SLAs) definieren und überwachen, die dem Schutzbedarf der IT-Komponenten entsprechen und innerhalb der Institution abgestimmt sind. Die festgelegten SLAs SOLLTEN die Rollen und Berechtigungen sowie eventuelle Abhängigkeiten der jeweiligen Tätigkeit von anderen Organisationseinheiten berücksichtigen.

OPS.1.1.1.A12 Spezifikation und Umsetzung klarer Betriebsprozesse (S)

Der IT-Betrieb SOLLTE für alle Aufgaben Betriebsprozesse spezifizieren, die für die jeweilige Aufgabe alle Tätigkeiten und Abhängigkeiten umfassen und gewährleisten, dass die Tätigkeiten des IT-Betriebs nachvollziehbar sind.

Es SOLLTE für jeden Prozess festgelegt werden, wer den Prozess initiieren darf und wer diesen umsetzt. Für jeden Prozess SOLLTEN die organisatorischen Schnittstellen zu anderen Gruppen des IT-Betriebs oder anderen Organisationseinheiten spezifiziert werden.

Das Personal des IT-Betriebs SOLLTE für die relevanten Betriebsprozesse eingewiesen werden.

Wenn Prozesse durchlaufen wurden, SOLLTE dies protokolliert werden. Das Ergebnis des Durchlaufs SOLLTE protokolliert werden. Für jeden Prozessschritt SOLLTE festgelegt werden, ob dokumentiert werden muss, dass er bearbeitet wurde. Darüber hinaus SOLLTE festgelegt werden, wann der Prozess erfolgreich abgeschlossen ist.

Der IT-Betrieb SOLLTE einen Prozess spezifizieren, der grundsätzlich beschreibt, wie mit Situationen umzugehen ist, die nicht in den regulären Betriebsprozessen enthalten sind. Mindestens SOLLTEN Fallback-Prozesse definiert sein und beschrieben werden, wie bei fehlerhaftem oder manipuliertem Betrieb vorzugehen ist.

OPS.1.1.1.A13 Absicherung der Betriebsmittel und der Dokumentation (S)

Auf die Betriebsmittel, die Dokumentation und die Betriebshandbücher SOLLTEN nur berechtigte Personen des IT-Betriebs zugreifen können. Der IT-Betrieb SOLLTE sicherstellen, dass die Betriebsmittel und die Dokumentation zu jeder Zeit verfügbar sind.

Falls die IT-Systeme und -Anwendungen der Betriebsmittel über die produktive Infrastruktur kommunizieren, SOLLTEN sichere Protokolle verwendet werden. Vertrauliche Daten SOLLTEN ausschließlich über sichere Protokolle übertragen werden.

Die Betriebsmittel SOLLTEN in das Schwachstellenmanagement und das IT-Monitoring eingebunden werden.

OPS.1.1.1.A14 Berücksichtigung der Betreibbarkeit bei Konzeption und Beschaffung (S)

Für die IT-Komponenten SOLLTEN Anforderungen für einen effizienten und sicheren Betrieb bereits bei der Konzeption und der Beschaffung berücksichtigt werden. Hierfür SOLLTEN die Anforderungen des IT-Betriebs erhoben und berücksichtigt werden. Der IT-Betrieb SOLLTE dabei auch die Komplexität der IT berücksichtigen.

OPS.1.1.1.A15 Planung und Einsatz von Betriebsmitteln (S)

Der IT-Betrieb SOLLTE für alle IT-Komponenten die Betriebsmittel bedarfsgerecht planen, beschaffen und einsetzen. Der IT-Betrieb SOLLTE die Anforderungen an die jeweiligen Betriebsmittel ermitteln und diese mit den anderen betroffenen Organisationseinheiten der Institution abstimmen.

Die Netze, in denen die Betriebsmittel positioniert sind, SOLLTEN von den sonstigen Netzen der Institution mindestens logisch getrennt werden (siehe Baustein NET.1.1 *Netzarchitektur und -design*). Das Netz für die Betriebsmittel SOLLTE abhängig von Sicherheitsrichtlinie und Funktionsabhängigkeiten weiter unterteilt werden. Als Basis für die weitere Segmentierung SOLLTEN die unterschiedlichen Betriebsgruppen und Zielsysteme verwendet werden.

OPS.1.1.1.A16 Schulung des Betriebspersonals (S)

Für den IT-Betrieb SOLLTE durch einen Schulungsplan sichergestellt werden, dass für alle IT-Komponenten und Betriebsmittel jeweils mehrere Personen die erforderlichen Fähigkeiten und Qualifikationen besitzen. In den Schulungsmaßnahmen SOLLTEN insbesondere die folgenden Themen adressiert werden:

- Härtung und Standard-Konfigurationen
- spezifische Sicherheitseinstellungen für die betriebenen IT-Komponenten und eingesetzten Betriebsmittel
- mögliche Interferenzen zwischen den genutzten Betriebsmitteln
- Abhängigkeiten und Schnittstellen der Prozesse des IT-Betriebs

Wenn neue IT-Komponenten beschafft werden, SOLLTE ein Budget für entsprechende Schulungsmaßnahmen des IT-Betriebs eingeplant werden.

OPS.1.1.1.A17 Planung des IT-Betriebs unter besonderer Berücksichtigung von Mangel- und Notsituationen (S)

Der IT-Betrieb SOLLTE für die betriebenen IT-Komponenten definieren, wann eine Mangel- oder eine Notsituation vorliegt. Für diese Situationen SOLLTE nach den Vorgaben des allgemeinen Notfallmanagements festgelegt werden, welche IT-Komponenten vorrangig betrieben werden oder für einen Mindestbetrieb benötigt werden. Die Notfallplanung SOLLTE die folgenden Punkte beinhalten:

- Disaster-Recovery-Plan
- Notfallhandbuch für die IT-Komponenten unter Einbeziehung der gesamten Infrastruktur
- Umgang mit kritischen und längerfristigen betriebsbehindernden Störungen

OPS.1.1.1.A18 Planung des Einsatzes von Dienstleistenden (S)

Der IT-Betrieb SOLLTE den Einsatz von Dienstleistenden koordinieren und diese unter anderem über SLAs so steuern, dass die Dienstleistung in ausreichendem Maße erbracht wird. Der Einsatz von verschiedenen Dienstleistenden SOLLTE aufeinander abgestimmt werden, insbesondere falls diese für den gleichen Tätigkeitsbereich vorgesehen sind. Für solche Situationen SOLLTE jeweils eine eindeutige Kommunikationsschnittstelle festgelegt werden.

Der IT-Betrieb SOLLTE die Festlegungen zum Dienstleistendenmanagement sowie die für die Dienstleistenden vorgesehenen Tätigkeiten festhalten, regelmäßig prüfen und anpassen.

OPS.1.1.1.A19 Regelungen für Wartungs- und Reparaturarbeiten (S)

IT-Komponenten SOLLTEN regelmäßig gewartet werden. Es SOLLTE geregelt sein, welche Sicherheitsaspekte bei Wartungs- und Reparaturarbeiten zu beachten sind. Es SOLLTE festgelegt werden, wer für die Wartung oder Reparatur von IT-Komponenten zuständig ist. Durchgeführte Wartungs- und Reparaturarbeiten SOLLTEN dokumentiert werden.

Es SOLLTE sichergestellt werden, dass Wartungs- und Reparaturarbeiten, die durch Dritte ausgeführt werden, mit den Beteiligten abgestimmt sind. Es SOLLTEN interne Mitarbeitende des IT-Betriebs bestimmt werden, die solche Arbeiten autorisieren, gegebenenfalls beobachten oder unterstützen und abnehmen.

OPS.1.1.1.A20 Prüfen auf Schwachstellen (S)

Der IT-Betrieb SOLLTE regelmäßig Informationen über bekannt gewordene Schwachstellen bezüglich der IT-Plattformen, Firmware, Betriebssysteme, eingesetzter IT-Anwendungen und Dienste einholen, diese für die konkreten Gegebenheiten analysieren und berücksichtigen.

Die IT-Komponenten SOLLTEN regelmäßig und anlassbezogen auf Schwachstellen getestet werden. Für jede IT-Komponente SOLLTEN die angemessene Test-Abdeckung, -Tiefe und -Methode festgelegt werden.

Die Tests und identifizierten Schwachstellen SOLLTEN nachvollziehbar erfasst werden. Die Schwachstellen SOLLTEN so schnell wie möglich behoben werden. Solange keine entsprechenden Patches zur Verfügung stehen, MÜSSEN für schwerwiegende Schwachstellen und Bedrohungen andere Maßnahmen zum Schutz der IT-Komponente getroffen werden. Falls dies für eine IT-Komponente nicht möglich ist, SOLLTE diese nicht weiter betrieben werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.1.A21 Einbinden der Betriebsmittel in das Sicherheitsmonitoring (H)

Die IT-Systeme und -Anwendungen, die als Betriebsmittel genutzt werden, SOLLTEN in ein Sicherheitsmonitoring eingebunden werden.

Falls die Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen einsetzt, SOLLTEN die Betriebsmittel darin eingebunden werden. Betriebsmittel wie IT-Management- und IT-Monitoring-Systeme SOLLTEN als Datenquelle für das Sicherheitsmonitoring genutzt werden.

OPS.1.1.1.A22 Automatisierte Tests auf Schwachstellen (H)

Alle IT-Komponenten SOLLTEN regelmäßig und automatisiert auf Schwachstellen getestet werden. Die Ergebnisse der Tests SOLLTEN automatisiert protokolliert und anderen Werkzeugen im Sicherheitsmonitoring bereitgestellt werden.

Bei kritischen Schwachstellen SOLLTE eine automatisierte Alarmierung erfolgen.

OPS.1.1.1.A23 Durchführung von Penetrationstests (H)

Für alle IT-Komponenten SOLLTEN Penetrationstests durchgeführt werden. Hierfür SOLLTE ein Konzept erstellt und umgesetzt werden, das neben den zu verwendenden Testmethoden und Testtiefen auch die Erfolgskriterien festlegt.

OPS.1.1.1.A24 Umfassendes Protokollieren der Prozessschritte im IT-Betrieb (H)

Für die Betriebsprozesse SOLLTE jeder Prozessschritt nachvollziehbar protokolliert werden.

OPS.1.1.1.A25 Sicherstellen von autark funktionierenden Betriebsmitteln (H)

Für die Betriebsmittel SOLLTE sichergestellt werden, dass diese auch bei äußeren Störungen genutzt werden können. Insbesondere SOLLTE eine ausgefallende Internet-Anbindung nicht zu einer Störung der Betriebsmittel führen.

Die Betriebsmittel SOLLTEN so konfiguriert und verortet werden, dass die Abhängigkeiten zwischen den verschiedenen Betriebsmitteln minimiert wird. Es SOLLTE verhindert werden, dass der Ausfall eines Betriebsmittels zu einer betriebsverhindernden Störung eines anderen Betriebsmittels führt.

OPS.1.1.1.A26 Proaktive Instandhaltung im IT-Betrieb (H)

Für die IT-Systeme SOLLTE eine proaktive Instandhaltung durchgeführt werden, in der in festgelegten Intervallen vorbeugende Instandhaltungsmaßnahmen durchgeführt werden.

Ergänzend zu der regelmäßigen Wartung und der proaktiven Instandhaltung SOLLTE je IT-Komponente abgewogen werden, ob eine vorausschauende Instandhaltung (engl. Predictive Maintenance) genutzt wird.

4. Weiterführende Informationen

4.1. Abgrenzung betriebsspezifischer Begriffe

Betriebshandbuch

Ein Betriebshandbuch (BHB) beschreibt je IT-Komponente alle relevanten Maßnahmen und Daten, die für den Betrieb der IT-Komponente notwendig sind. Ein BHB basiert auf dem entsprechenden Betriebskonzept und ist als lebendes Dokument zu betrachten, das fortwährender Aktualisierung und Ergänzung unterliegt.

Betriebskonzept

Ein Betriebskonzept beschreibt für eine gleichartige Gruppe von IT-Komponenten die Betriebsorganisation und die Betriebsprozesse. Das Betriebskonzept bildet die Grundlage für das Betriebshandbuch.

Betriebsprozesse

Ein Betriebsprozess spezifiziert die Tätigkeiten, die zur Erfüllung einer Betriebsaufgabe notwendig sind. Komponentenspezifische Betriebsprozesse können auch als Teil des Betriebshandbuchs definiert werden.

4.2. Wissenswertes

Die Information Technology Infrastructure Library (ITIL) gibt Hinweise (Best Practices) zur Einrichtung und Umsetzung des Service Management einer Institution.

Die International Organization for Standardization (ISO) spezifiziert in der Norm ISO/IEC 20000 die Mindestanforderungen an Prozesse des IT Service Management, um einen messbaren Qualitätsstandard der IT-Services zu gewährleisten. Die Norm ISO/IEC 20000 ist an ITIL ausgerichtet und ergänzt deren Best Practices.